AMENDMENTS TO THE SPECIFICATION

Amend the paragraph from page 3, lines 1-11 as follows:

A method used for an illegal intrusion will now be described while referring to Fig. 1. In the schematic diagram in Fig. 1, an attacker's computer 11 is used to effect an illegal intrusion of a targeted host 16 via a plurality of host computers 12 to 15, and a network 17 to which these computers are connected. In this setup, the routing of packets on the network 17 is controlled by a router 18. So in order to hide his or her identity ~~identify~~, the attacker, hereinafter referred to as the attacker 11, attacks the target host 16 via one or more of the stepping-stone computers 12 to 15.

Amend the paragraph found on page 18, lines 8-27 as follows:

The structure of an IP header will be described while referring to Fig. 6. The horizontal axis represents bits, and for every 32 bits (4 bytes) there is a line return, the line continuing at a location all the way to the left and one space below the previous line. Along the same line, a left bit represents an upper bit. A normal IP header with no Options is 20 bytes from Version to Destination Address. The Source Address and the Destination Address are respectively ~~the respective~~ the IP address of the transmission source apparatus and the IP address of the destination (reception) apparatus. Fig. 7 is a diagram showing the structure of the TCP packet in the same manner as in Fig. 6. The normal TCP header with no Options and data is 20 bytes from Source Port to Urgent Pointer. The Source Port, the Destination Port and the Sequence Number are, respectively, the port number of the transmission source apparatus, the port number of the destination (reception) apparatus and a number provided for each packet at one connection. Since these data structures are well known, no detailed explanation will be given for them.

Amend the paragraph found from page 21, line 29 through page 22, line 15 as follows:

The log box selects desired packet data from those recorded in the recording unit 54. Basically, a connection can be specified by using the four indicators (the source IP address, the source port number, the destination IP address and the destination port number) that are extracted from the IP header and the TCP header of a packet. Thus, whether the individual packet data sets are included in the connection used by the attacker can be determined. Therefore, packet data whose indicators match are written in the file. The packet data written in the file has the same form as the packet data recorded by the recording unit 54. The data file is then distributed to each site together with a packet requesting ~~the~~ that a search be performed. The distributed packet and the data file are received by the log box at each site, and the individual log boxes activate comparison determination programs.

Amend the paragraph found from page 31, line 11, through page 32, line 1 as follows:

The log boxes at ~~of~~ the individual sites select several series whose similarities, obtained using the above calculation, are equal to or smaller than a predetermined value. The selected series and the connections including these series and the similarities are returned to a request source site. Upon the receipt of these data from the sites, the requesting site finds a connection having an especially high similarity, which is probably a connection on the same chain. Further, the requesting site communicates with the managers of the hosts, confirms that the hosts were used as stepping stones by the attacker, and finally begins tracing manually. While taking into account the fact that the attacker may intrude on the system again, a PC for recording packet data is installed for the backbone of the network to which the IP address, which is one of the four elements of the connection that exhibits the most similarity, so that the monitoring performed to detect the attacker can be thereafter improved.